Sempre Pronto!

POLÍTICA DE GESTÃO DE RISCOS

Versão: 1.0

Aprovação: Conselho de Administração

Revisão: anual ou sempre que houver atualização normativa relevante

1. OBJETIVO

Esta Política estabelece os **princípios, diretrizes e responsabilidades** da Pronto! Serviços de Pagamento Ltda. para a **identificação, avaliação, monitoramento, mitigação e reporte de riscos** inerentes às suas atividades, assegurando que a instituição mantenha níveis de risco compatíveis com seu **apetite e tolerância definidos pela administração**, em conformidade com as normas regulatórias.

2. ABRANGÊNCIA

Esta Política aplica-se a **todas as áreas, unidades de negócio, colaboradores, administradores, fornecedores e parceiros** que participem, direta ou indiretamente, das operações e serviços de pagamento oferecidos pela Pronto!

A estrutura de gestão de riscos abrange os riscos **estratégicos, operacionais, financeiros, de conformidade, cibernéticos, de liquidez, crédito, mercado e reputacionais**, conforme classificação definida nesta política.

3. GLOSSÁRIO

Apetite ao Risco: nível de risco que a Pronto! está disposta a aceitar para atingir seus objetivos estratégicos, em conformidade com sua estrutura de capital e perfil regulatório.

Tolerância ao Risco: variação aceitável em relação ao apetite ao risco definido.

Gestão de Riscos: conjunto de políticas, processos e estruturas para identificar, mensurar, tratar e monitorar riscos, conforme diretrizes da **ISO 31000** e do **COSO ERM**.

Risco: possibilidade de ocorrência de evento que impacte negativamente o alcance dos objetivos estratégicos, financeiros, operacionais ou de reputação.

KRI (Key Risk Indicator): indicador-chave que sinaliza variações relevantes no nível de exposição ao risco.

KPI (Key Performance Indicator): indicador de desempenho que mede a efetividade das ações de mitigação.

RTO (Recovery Time Objective): tempo máximo aceitável de recuperação de processo crítico após interrupção.

RPO (Recovery Point Objective): perda máxima aceitável de dados em caso de incidente.

4. DIRETRIZES GERAIS

A Pronto! mantém um **Sistema Integrado de Gestão de Riscos (SIGR)** baseado nas **melhores práticas internacionais e nas exigências regulatórias do Banco Central do Brasil**, em especial as **Resoluções CMN nº 4.557/2017 e nº 4.595/2017**, que dispõem sobre a estrutura de gerenciamento de riscos e controles internos.

A política é parte integrante do **Programa de Compliance e Governança Corporativa da Pronto!**, e orienta o funcionamento da **função de riscos**, garantindo independência, autonomia técnica e reporte direto à Alta Administração e ao Conselho de Administração.

5. OBJETIVOS DA GESTÃO DE RISCOS

A gestão de riscos da Pronto! visa:

- **Aumentar a probabilidade de alcance das metas estratégicas**;
- **Identificar oportunidades e ameaças** que possam afetar o negócio;
- **Aprimorar a transparência e a prestação de contas** junto às partes interessadas;
- **Atender às exigências legais e regulatórias**, especialmente do Bacen e da LGPD;
- **Melhorar a qualidade e a agilidade na tomada de decisão**;
- **Otimizar a alocação de capital e recursos**;
- **Reduzir perdas financeiras, operacionais e reputacionais**;
- **Fortalecer a resiliência organizacional** e a prontidão para eventos disruptivos

6. CLASSIFICAÇÃO E TIPOLOGIA DOS RISCOS

A Pronto! adota estrutura de classificação baseada nas normas e **Res. CMN 4.557/2017**, contemplando os seguintes tipos de risco:

i. **Risco Estratégico:** associado a decisões de negócio, ambiente macroeconômico e fatores externos.

ii. **Risco Operacional:** proveniente de falhas em processos internos, pessoas, sistemas ou eventos externos.

iii. **Risco de Conformidade:** resultante de descumprimento de normas legais, regulatórias ou internas.

iv. **Risco Cibernético e de Segurança da Informação:** relacionado a acessos não autorizados, ataques cibernéticos ou perda de confidencialidade, integridade e disponibilidade de dados.

v. **Riscos Financeiros:**

   a. **Risco de Crédito:** inadimplência ou deterioração da qualidade do crédito concedido.

   b. **Risco de Mercado:** variação adversa em taxas de juros, câmbio ou preços.

   c. **Risco de Liquidez:** incapacidade de honrar compromissos financeiros.

vi. **Risco Reputacional:** impactos negativos à imagem ou confiança na instituição.

vii. **Risco Socioambiental e ESG:** exposição a danos ambientais, sociais ou de governança corporativa.

7. ESTRUTURA DE GOVERNANÇA E RESPONSABILIDADES

A estrutura de governança da Pronto! segue o modelo das **Três Linhas de Defesa**, conforme diretrizes do **Institute of Internal Auditors (IIA)** e do **Banco Central do Brasil**:

1ª Linha – Áreas de Negócio e Operações

- Identificar, avaliar e mitigar riscos diretamente relacionados às suas atividades;
- Implementar e manter controles operacionais;
- Reportar incidentes, eventos e fragilidades à área de Riscos e Compliance.

2ª Linha – Funções de Controle (Riscos, Compliance e Jurídico)

- Coordenar a gestão integrada de riscos e compliance;
- Definir metodologias, limites, matrizes de risco e relatórios de monitoramento;
- Garantir aderência à regulação vigente e às políticas corporativas;
- Reportar periodicamente ao Comitê de Riscos e à Alta Administração.

3ª Linha – Auditoria Interna

- Avaliar, de forma independente, a eficácia da estrutura de riscos e controles internos;
- Emitir recomendações e acompanhar planos de ação corretiva;
- Reportar diretamente ao Conselho de Administração ou Comitê de Auditoria.

8. PROCESSO DE GESTÃO DE RISCOS

O processo de gestão de riscos segue as etapas da **ISO 31000**, em ciclo contínuo (PDCA):

1. **Identificação:** levantamento de riscos inerentes e residuais por processo, produto e serviço;
2. **Análise e Avaliação:** classificação quanto à probabilidade e impacto (baixo, médio, alto);
3. **Tratamento:** definição de estratégias (aceitar, mitigar, transferir ou eliminar o risco);
4. **Monitoramento:** acompanhamento contínuo por meio de indicadores (KRIs e dashboards);
5. **Comunicação e Reporte:** emissão de relatórios de risco à Alta Administração e aos órgãos de governança.

9. FERRAMENTAS E MECANISMOS DE APOIO

Para assegurar uma gestão robusta, a Pronto! utiliza:

- **Matriz de Riscos Corporativos (Heat Map)** com avaliação periódica;
- **Sistemas automatizados de monitoramento e alertas**;
- **Análises de cenários e testes de estresse** (stress testing);
- **Indicadores de risco (KRIs)** e **indicadores de desempenho (KPIs)**;
- **Monitoramento contínuo de transações e fraudes**;
- **Dashboards e painéis executivos em tempo real**;
- **Integração com o Plano de Continuidade de Negócios (PCN)** e o **Programa de Compliance**

10. POLÍTICA DE DADOS E LGPD

Todas as atividades de gestão de riscos observarão os princípios da **Lei nº 13.709/2018 (LGPD)** e demais normas de privacidade, garantindo:

- O tratamento adequado e seguro de dados pessoais;
- A observância dos princípios de finalidade, necessidade e transparência;
- O uso de dados apenas para fins legítimos de análise de risco;
- A comunicação imediata de incidentes de segurança ao Encarregado (DPO) e, quando aplicável, à ANPD.

11. CANAIS DE ATENDIMENTO E REPORTE

Para dúvidas, comunicações ou reportes relacionados à Política de Gestão de Riscos:

- **E-mail:** compliance@sempreprontto.com.br
- **Ouvidoria**: ouvidoria@sempreprontto.com.br

12. DISPOSIÇÕES FINAIS

- Esta Política é **de caráter público** e reflete o compromisso institucional da Pronto! com a **transparência e solidez de sua estrutura de gestão de riscos**;
- As violações às diretrizes aqui estabelecidas serão tratadas como **não conformidades**, sujeitas a sanções administrativas ou disciplinares;
- A Política será **revisada anualmente** ou sempre que houver alterações significativas na estrutura de risco, estratégia corporativa ou regulação vigente;
- Casos omissos serão analisados pela **Área de Riscos e Compliance**, com deliberação final pela **Alta Administração**.